Good morning, Mr. Chairman. I am pleased to have this opportunity to appear before the Committee and talk about the role that the Department of Justice is playing to combat Internet fraud, with particular regard to senior citizens.

BACKGROUND

There is no question that the Internet has become increasingly attractive to all segments of the population as a medium for everyday information-gathering, communication, and commercial activity. A 2003 report by the Pew Internet and American Life Project shows how popular the Internet has become. As of August 2003, 63 percent of all adult Americans – 126 million people -- now go online, and 52 percent of those Internet users – 66 million people -- go online on a typical day. Older adults are a significant component of this growth. In August 2003, according to the Pew Internet Project, 59 percent of people age 50 to 64, and 22 percent of people age 65 and older, had become Internet users, and those numbers will continue to increase.

It is also important to note the types of online activities in which Internet users routinely engage. For example, according to the Pew Internet Project, online auction participants have almost doubled since 2000 – from 13 million bidders and purchasers in March 2000 to nearly 24 million by December 2002. In addition, the number of people who have tried some form of online banking increased by 127 percent from March 2000 to October 2002, the number of people who have made purchases online has increased by 63 percent since 2000, and about one in ten Internet users has bought or sold stocks online. Finally, the number of Internet-using seniors who search for health information online or do online banking has increased by 20 percentage points since 2000.

Not surprisingly, law enforcement in recent years has witnessed a corresponding growth in online criminal fraud. The Federal Trade Commission (FTC), which receives complaints on

both identity theft and Internet fraud, has noted that the numbers and percentages of identity theft complaints and Internet fraud complaints filed with the FTC have increased greatly in the past three years. Identity theft complaints have nearly tripled in the past three years, from 86,212 in 2001 – 39 percent of all complaints filed with the FTC – to 214,905 – 42 percent of all complaints -- in 2003. It is important to note that identity theft now includes such online criminal techniques as "phishing" – schemes in which criminals set up emails and websites designed to look like those of legitimate companies and financial institutions, then induce people to disclose bank and financial account data, as well as personal data, that can be used in identity theft and fraud. I understand that David Jevans of the Anti-Phishing Working Group will discuss phishing schemes in greater detail in his testimony today.

Internet-related fraud complaints filed with the FTC have also tripled, from 55,727 complaints (42 percent of all complaints) in 2001 to 166,617 complaints (55 percent) in 2003. Both the FTC and the Internet Crime Complaint Center – a joint venture of the FBI and the National White Collar Crime Center -- report that Internet auction fraud has remained the most frequently reported type of online fraud. The Internet Crime Complaint Center reported in 2002, for example, that auction fraud accounted for 46.1 percent of all fraud complaints that it referred to law enforcement.

Other types of online fraud capable of harming seniors have also remained highly prevalent. For example, the Internet Crime Complaint Center reported in 2002 that non-delivery of merchandise or payment for goods ordered online made up 31.3 percent of all referred fraud complaints. We also understand that the Securities and Exchange Commission's Office of Internet Enforcement receives an average of approximately 1,000 complaints per business day.

While a substantial number of these complaints involve non-Internet-related securities fraud, many complaints stem from large-scale spamming of fraudulent or questionable securities-related e-mails to prospective investors in all demographic segments.

At present, our prosecutions of Internet fraud cases indicate that the people behind the schemes range from individuals with no prior criminal records to organized groups, both domestic and international in scope. Although we are not aware of specific cases in which traditional organized crime groups such as La Cosa Nostra or motorcycle gangs organized or conducted the schemes, federal law enforcement is continuing to watch closely for any indications that such groups are becoming involved in online fraud.

DEPARTMENT OF JUSTICE PROSECUTION OF INTERNET FRAUD

The Department of Justice is strongly committed to combating all forms of Internet fraud, and to protecting senior citizens from criminals who may seek to target them for any type of fraud. It should be noted that investigation of any Internet fraud scheme, including those affecting seniors, often must overcome several challenges in order to make prosecution of the offenders possible. Investigators, first of all, must amass evidence that makes it possible to attribute behavior, including criminal behavior, to individuals. This task is often a formidable one because of the technology of the Internet, which can enable criminals to conduct their activities with anonymity. Second, the global reach of the Internet not only enables criminals to conduct schemes across multiple jurisdictions, but complicates the task of finding and accessing relevant evidence from those jurisdictions. For example, nearly one-fourth (23.3 percent) of the Internet fraud perpetrators identified by the FBI in 2002 were located outside the United States. Third, investigators must be able to locate and obtain Internet-related evidence quickly, as

critical evidence in the possession of Internet service providers and other e-commerce companies may be preserved for only short spans of time. Fourth, even after they have obtained access to relevant electronic data, the sheer volume of those data may enhance the difficulty of finding the most probative evidence among those data.

I should also note that, as more seniors become computer literate and go online, those seniors who are relative novices are, of course, more susceptible to computer crimes, other than fraud, based on computer intrusions. Their computers may be compromised by hackers who want to steal their data, hijack their computers in order to churn out spam, launch denial of service attacks against others, or carry out other crimes. In addition, seniors who are novice computer users may be more vulnerable to viruses and worms and may, unwittingly, contribute to the spread of such malicious code. These issues involving seniors and the Internet are also concerning.

As part of our coordinated efforts to combat Internet fraud, since 2001 the Department, in coordination with the FBI, the Postal Inspection Service, the Federal Trade Commission, and other law enforcement agencies, has conducted three nationwide "takedowns" of Internet fraud cases. The first of these takedowns, "Operation Cyber Loss" in 2001, involved investigations of online fraud schemes in which more than 56,000 victims lost more than $117 million, and resulted in criminal charges against approximately 90 individuals and companies. In May 2003, we announced the take-down of Operation E-Con, which involved more than 90 investigations of fraud schemes in which 89,000 victims lost an estimated $176 million, and led to the arrests or conviction of more than 130 individuals. Most recently, in November 2003, Operation Cyber

Sweep involved the arrests or convictions of more than 125 individuals and the return of more than 70 indictments directed at some of the leading types of online economic crime.

These takedowns included prosecutions of large-scale Internet fraud schemes involving bogus investments, "phishing" schemes and other identity theft, online auction frauds, and other cases in which senior citizens and others were at risk of loss or harm. Here are a few examples of these prosecutions:

Online Investment Fraud

One type of online fraud that poses a particular threat to seniors is investment fraud. Seniors seek financial information on-line more than any other group of Internet users. And seniors who entrust substantial funds to a fraudulent investment opportunity not only lose savings that may be essential for their current needs, but often have fewer opportunities and less time to recoup those funds. Indeed, the proportion of individuals who report losses of more than $5000 from Internet fraud is highest for those age 60 and older.

As part of Operation E-Con in 2001, the United States Attorney's Office for the Eastern District of California indicted two defendants on fraud- and money laundering-related charges relating to one of the largest Internet investment fraud cases in the country. The Tri-West Investment Club was an Internet-based investment fraud scheme that netted approximately $60 million from 15,000 investors worldwide. Tri-West solicited investments in what the website termed a "Bank Debenture Trading Program" or "Prime Bank" note program. The website guaranteed investors a 120 percent annual rate of return with "no risk of losing the investor's principal investment," as well as substantial referral fees for directing others to the website. The case alleged that these investment instruments were nonexistent. According to the indictment,

Tri-West never actually invested any of the investors' money in any "prime bank note" program, but instead used new investor funds to make "dividend" payments to earlier investors to give the false impression of profitability – a classic Ponzi scheme. The balance of the funds were used by the two defendants and others to purchase millions of dollars of real properties in Mexico and Costa Rica, as well as a yacht and helicopter, and to funnel money to dozens of shell companies created in Costa Rica to conceal the defendants' ill-gotten gains.

The indictment also sought the forfeiture of millions of dollars of real properties in Costa Rica and Mexico, a yacht, a helicopter, over a dozen cars, and millions of dollars in bank accounts in Latvia, Mexico and Costa Rica. The two defendants, who were extradited from Costa Rica to Sacramento in December 2002 to face federal charges, have since pleaded guilty, are cooperating with authorities, and remain in custody pending sentencing. A third defendant, Cary Waage, pleaded guilty in 2002 to separate charges relating to Tri-West, is cooperating with authorities and remains in custody pending sentencing. Other individuals allegedly connected with the operations of Tri-West remain fugitives.

Another Operation E-Con case involved a prosecution by the United States Attorney's Office for the District of Colorado. In this case, the defendant was indicted on 15 fraud-related counts pertaining to his alleged operation of an Internet-based Ponzi scheme that took in more than $8 million from 23,000 investors. The defendant allegedly used a website to offer investors an opportunity to become "members" of an offshore investment program run by a company called J&K Global Marketing Corporation. He allegedly promised that if an investor paid a yearly "membership fee" of $375 and waited six months, he or she would receive payments of $375 per month. He also allegedly told investors that he was investing in "high-yield programs,"

which would return between 200 percent and 1200 percent per month. As a result, investors allegedly transmitted membership fees to bank accounts in the United States, Canada, Luxembourg, and the West Indies. The defendant has since agreed to plead guilty and is expected to enter his plea next month.

"Phishing" Schemes and Other Identity Theft

Another type of fraud-related crime that may have special impact on seniors is identity theft. Because they often have accumulated substantial financial assets during their years of employment, seniors may have bank and other financial accounts that criminals can easily drain once they have obtained personal and financial data from those seniors through identity theft. Moreover, because many seniors have paid off their mortgages and buy new cars less frequently, they may be less likely to order or review their credit reports in connection with a home refinancing or large-scale consumer purchase. This means that they may be less likely than some younger homeowners and consumers to detect that they have become identity theft victims.

In Operation E-Con, the United States Attorney's Office for the District of Maryland obtained an indictment against two defendants for devising and executing a scheme to lure unsuspecting bank customers to "spoofed" bank websites. At these websites, customers would enter confidential account data that would be transmitted to the defendants, who would use the data to produce and fraudulently use ATM and credit cards. One of these defendants, whose case was transferred to the District of Connecticut, pleaded guilty to bank fraud and wire fraud charges and is awaiting sentencing. The other defendant, a foreign national, is a fugitive – again demonstrating the trans-national nature of these cases.

In another E-Con case, the United States Attorney's Office for the Western District of Pennsylvania obtained an indictment against a defendant on charges of conspiracy, bank fraud, and access device fraud. According to the indictment, the defendant fraudulently used the names, Social Security numbers, and other identifying information from two individuals to apply over the Internet to obtain bank loans and credit cards in the other people's names, and made fraudulent online purchases. On May 23, 2003, the defendant was sentenced to 21 months imprisonment and approximately $25,000 in restitution.

In Operation Cyber Sweep last year, the United States Attorney's Office for the Eastern District of Virginia obtained a guilty plea from a woman on charges of conspiracy to possess unauthorized access devices. The defendant had engaged in "phishing" by sending fake e-mail messages to America Online (AOL) customers, advising that they must update their credit card/personal information on file with AOL to maintain their accounts. Unwitting victims provided their information to the defendant and her co-conspirators. Subsequently, the defendant was sentenced to 46 months imprisonment. One of her co-conspirators previously had pleaded guilty to the same charge and was sentenced to 37 months imprisonment.

In a second Cyber Sweep case, the United States Attorney's Office for the Southern District of New York obtained guilty pleas from two individuals to charges of conspiracy and identity theft for their roles in an Internet fraud scheme that exploited the online payment service PayPal and financial institutions. The defendants and their co-conspirators stole banking and pedigree information from one of their employer's payroll office. They then used the information to open PayPal accounts, and fund the PayPal accounts by direct transfers from the victims' bank accounts to PayPal. Thereafter, they used the fraudulently-funded PayPal

accounts to purchase various items on eBay, and then they sold many of those items on eBay for cash. One defendant pleaded guilty to conspiracy and access device fraud charges on January 23, 2004, and was sentenced to 30 months imprisonment. The other defendant also pleaded guilty to conspiracy and access device fraud charges on October 10, 2003, and is scheduled to be sentenced next month.

In a third Cyber Sweep case, the United States Attorney's Office for the Eastern District of Michigan obtained a criminal complaint and arrest of an individual for credit card fraud, where the Internet was allegedly used to order more than $9,000 in airline tickets. The defendant was a former hotel desk clerk who had access to hotel guests' credit-card numbers and other personal data. The tickets were allegedly purchased using stolen credit-card information from 12 victims using Expedia.com and Lodging.com. The investigation of this case is continuing.

Online Auction Frauds

One of the most common types of Internet fraud involves online auctions. While only a small proportion of seniors (15 percent) who use the Internet report engaging in such auctions, those who do remain vulnerable to this type of crime.

In Operation E-Con, the United States Attorney's Office for the Western District of Pennsylvania obtained a plea of guilty from a defendant to a charge of conspiracy to commit mail fraud and wire fraud. The defendant, who was originally from Belarus, participated in a mail and wire fraud scheme that had two interconnecting parts. The first part of the scheme was that members of the conspiracy hacked into eBay's computer system and logged onto the system as if they were someone who had previously sold items and received favorable ratings from

purchasers of those items. Once a seller received a favorable rating, it was much easier to sell items because there was a proven track record of delivering what was promised.

Members of the scheme then put items up for auction pretending that they were sellers with the proven track records. The successful bidder in the auction was directed to send certified checks or money orders to an address in Pennsylvania, but no items were delivered. The second part of the scheme involved the unauthorized use of credit card numbers to purchase items online that were then shipped to addresses in Pennsylvania. These items were then repackaged and sent to addresses in California. The addresses in Pennsylvania were set up by two co-conspirators, also originally from Belarus, who used false identifications. These two individuals, who worked under the defendant's direction, would stay in apartments for approximately two weeks at a time and receive products and checks at those locations. They would then move to a different apartment and, again, receive checks and products. They moved to a total of four different apartments during the course of the conspiracy until they were arrested by the Pennsylvania State Police. On July 10, 2003, the defendant was sentenced to 18 months imprisonment.

In Operation Cyber Sweep, the United States Attorney's Office for the Eastern District of Missouri obtained an indictment against three individuals for conspiracy to commit wire fraud. According to the indictment, between October 2, 2002 and February 13, 2003, the three defendants monitored Internet-based auctions for sporting event and concert tickets on systems such as eBay and identified losing bidders. Thereafter, one or more of the defendants would send a form letter e-mail message to losing bidders informing them of the availability of additional tickets and inviting those bidders to purchase such tickets from one of them. When a bidder responded to an e-mail invitation to purchase tickets, the bidder was instructed how to pay

for the tickets, typically by way of a Western Union money transfer. In other cases, one or more of the defendants fraudulently solicited bids for event tickets using auctions on eBay. Winning bidders were typically notified by e-mail that the winning bidder was required to make a substantial payment of funds, typically by way of a Western Union transfer of money, before any tickets would be delivered. The indictment further alleged that, upon receipt of money from a bidder, the defendants would keep the proceeds but did not deliver tickets to the bidder. The events included tickets for a Bruce Springsteen concert, tickets for the Fiesta Bowl, tickets for the 2002 SEC Championship football game, and tickets for a Los Angeles Lakers basketball game. All three defendants have since pleaded guilty to the indictment and are scheduled for sentencing next month.

Online Pharmaceutical Sales

The Department of Justice has brought a number of criminal prosecutions against individuals who engage in fraudulent sales of drugs and medical devices that may put senior citizens at risk. A very high proportion – 74 percent – of seniors who use the Internet seek health information on-line. Because seniors are highly sensitive to the cost of prescription drugs, seniors may be especially vulnerable to websites or emails that falsely claim to offer safe and effective drugs at what seniors consider affordable prices. Moreover, in some cases senior citizens may be disproportionately harmed if they seek to purchase needed drugs or medical supplies from fraudulent websites.

In Operation Cyber Sweep, the United States Attorney's Office for the Middle District of Louisiana obtained an indictment against a college student on charges of wire fraud relating to his alleged online sales of prescription drugs. The indictment alleges that the defendant,

utilizing the email address Hydrocodone@anywhereUSA.com, posted several messages on a bulletin board owned by www.healthboards.com advertising the sale of prescription pain pills. In February 2003, an FBI agent, acting in an undercover capacity, began sending e-mails to the defendant and arranged to purchase Morphine, Oxycodone, Hydrocodone, Skelaxin and Percocet. The agent wired the funds to purchase the drugs to the defendant from a local convenience store in Baton Rouge and requested that the drugs be sent to him in Baton Rouge. The defendant and another individual went to the Western Union Office in Moscow, Idaho and picked up the funds, but the defendant never sent the drugs ordered by the undercover agent. The case was subsequently transferred to the District of Idaho, where the defendant has pleaded guilty and is scheduled to be sentenced this week.

Just last week, the United States District Court for the Eastern District of Virginia sentenced a pharmacist to 60 months imprisonment and a $140,318 fine for conspiring to violate the Controlled Substances Act and the Federal Food, Drug, and Cosmetic Act in connection with the illegal sale of controlled substances and other prescription drugs over the Internet to consumers through various websites.

* * * * *

There are at least five factors have made it possible for the Department to bring so many successful prosecutions against various forms of Internet fraud. First, several provisions in the Federal Sentencing Guidelines make it possible, in fraud cases involving seniors, to seek higher sentences. Under Section 3A1.1 of the Guidelines, for example, a defendant may receive a two-level increase if he knew or should have known that a victim was unusually vulnerable or otherwise susceptible to the criminal conduct. This enhancement may apply in online

investment schemes, where seniors and others may be susceptible to promises of financial security. [*See* United States v. Harris, 38 F.3d 95 (2d Cir. 1994), cert. denied, 513 U.S. 1198 (1995).] Under Sections 2B1.1 and 3A1.1, respectively, the Department may seek additional enhancements where a substantial part of the scheme was committed from outside the United States or where large numbers of vulnerable victims were involved.

Second, the Department has an ongoing Internet Fraud Initiative that, among other things, ensures that federal prosecutors and agents receive appropriate training about Internet fraud. The Department's National Advocacy Center conducts basic courses in cybercrime that include training about Internet fraud, as well as more advanced courses that focus exclusively on Internet fraud. The Department also supports investigative agencies' in-service training about Internet fraud by providing speakers from the Department's Criminal Division and various United States Attorneys' Offices.

Third, as part of the Internet Fraud Initiative, the Department plays an important role in fostering national-level and cross-border cooperation among law enforcement agencies, by convening and chairing interagency working groups. At the national level, the Telemarketing and Internet Fraud Working Group includes the Postal Inspection Service, the FTC, and the North American Securities Administrators Association, as well as the FBI, the U.S. Secret Service, and other federal and state law enforcement organizations. In the Waage investment fraud case I discussed earlier, the contacts that this Working Group has developed made possible rapid and effective coordination between state securities administrators, the Securities and Exchange Commission, the FBI, and the United States Attorney's Office for the Eastern District of California in the criminal investigation and prosecution. At the international level, the

Department co-chairs the United States - Canada Working Group on Cross-Border Mass-Marketing Fraud, which facilitates similar coordination between U.S. and Canadian law enforcement agencies.

Fourth, the Department recognizes that the successes of initiatives such as E-Con and Cyber Sweep depend heavily on the Department's maintaining close and effective coordination with other federal agencies, such as the FTC and the Postal Inspection Service, on Internet fraud matters. We value our partnerships with the FTC and the Postal Inspection Service in combating Internet fraud and other forms of mass-marketing fraud, such as cross-border telemarketing fraud schemes that target seniors.

Finally, in these Internet fraud takedowns, federal law enforcement has benefitted substantially from cooperation and coordination with foreign governments and the private sector. In the Waage investment fraud case, Costa Rican government authorities made significant contributions in gathering evidence and conducting searches and seizures of property, as well as extraditing defendants. In Operation Cyber Sweep, law enforcement authorities in Ghana and Nigeria and the Merchants Risk Council provided significant assistance to the FBI and other investigative agencies in a number of cases. In 2004, the Department has expanded its outreach to and coordination with the private sector on issues such as "phishing" schemes, and, together with the FBI, the U.S. Secret Service, and the Federal Deposit Insurance Corporation, have been participating in meetings with the Anti-Phishing Working Group.

As important as our enforcement efforts are in combating Internet fraud, the Department also recognizes that continuing public education and prevention measures are needed to warn the public, including senior citizens, about various types of Internet fraud. The Department's own

website, www.usdoj.gov, includes a recently posted Special Report about "phishing" schemes (at http://www.usdoj.gov/criminal/fraud/Phishing.pdf), as well as other Special Reports on identity theft and Africa-related email solicitations and an extensive set of webpages on Internet fraud. The Department also strongly supports the FTC's and the Postal Inspection Service's public education and prevention measures affecting Internet fraud, such as the extensive webpages and printed materials they provide to the public on identity theft and consumer frauds.

* * *

Mr. Chairman, that concludes my prepared remarks. I would be happy to take questions from the Committee at this time.